UNCLAS
Information Paper
5 November 2010

Subject: Army Mandate for Immediate Migration of Single Sign On to DOD PKI Based Authentication

Purpose: To provide awareness and timelines of the Army CIO/G6 Policy for enforcing the migration of Army Knowledge Online (AKO) Single-Sign-On (SSO) to DOD PKI based authentication in compliance with DoD Policy Joint Task Force Global Network Operations Communications Task Order 07-15 (JTF-GNO CTO 07-15).

Background: The Army has not been compliant with JTF-GNO CTO 07-15 nor its predecessor JTF-GNO 06-02.

a. JTF-GNO CTO 07-15 identified:
   i. username/passwords as a security vulnerability ;
   ii. Outlined specific tasks to include PK-enabling users, systems, and issuing alternate smart card login for privileged level users
b. JTF-GNO CTO 06/02 applies to:
   i. PK-enabling enclaves, desktops, servers, and laptops that connect to the NIPRNET;
   ii. Eliminating all username/passwords and non-DoD PKI certificate authorities;
   iii. Permitting only certificate-based client authentication to Private DOD Web servers using certificates issued by DOD PKI certificate authorities.

Mandate to Action: In a policy memorandum dated 28 October 2010, Army CIO/G6 directed for immediate action the migration of Army Knowledge Online (AKO) Single Sign-On (SSO) to DOD PKI based authentication in compliance with DOD Policy (JTF-GNO CTO 07-15). Utilizing CAC/PKI significantly decreases the threat to Army IT systems (AIS) and networks.

To secure access to AIS, the CIO/G6 directs:

(a) All applications and devices will be configured to only allow authentication via CAC/PKI credentials for CAC holders.
(b) All AIS currently using username/password and passwords via AKO for authentication must convert to PKI-based authentication for CAC holders.
(c) Family members and Retirees will continue to access IT systems via usernames/passwords per AR 25-1.
(d) No later than 1 December 2011, the Army will implement the Enterprise User Name Standard and enforce CAC only authentication to enterprise email, web services, and applications.
(e) All systems and applications that cannot achieve full CAC/PKI login by 1 December 2011:
   i. Submit to CIO/G6 an individualized Plan of Action and Milestones (POA&M) by 31 January 2011.
   ii. POA&M must include details of how and when the systems and applications will become compliant no later than 1 December 2011.

Impact to AG1-CP Systems, Servers, Applications and Recommendation:

a. Certain AG-1 CP systems have been designed and are dependent on AKO SSO for access and authentication.

b. In order to become fully compliant with DoD Policy JTF GNO 07-15 and Army directives, all access must be PKI enabled effective 1 December 2011.
c. All Systems, Servers, and applications planned for deployment and which are dependent on Army or DoD Enterprise services must be enabled;
d. All Systems, Servers, and applications planned for deployment and which are dependent on Army or DOD Enterprise services but are planned for conversion to CAC/PKI login **will lose access** to the private (FOUO) network.

Recommendation: Recommend owners of AG-1 CP Systems, Servers, and Applications who are unable to comply with the mandate submit POA&Ms to CIO/G6 (GACKO.Actions.AO@us.army.mil) by 31 January 2011 as directed.

Detailed guidance (including instructions and templates) for achieving a successful conversion from SSO to DOD PKI based authentication has been published to: https://www.us.army.mil/suite/page/641492.

Provided by Joudi M. Henoud, CISSP
CISTO Team/Lockheed Martin/AG-1 CP/ CISD-IA Team Lead
703-325-4682